CLAIMS
What is claimed is:

1.   A method of controlling access to a website, the method comprising:

      receiving a request for a web page from a client computer;

5   searching the client computer for a pass to the website; and

      if the client computer does not have a pass to the website, setting a blocking

layer having an opaque portion over the website such that an end-user on the client

computer cannot interact directly with the website.

2.   The method of claim 1 further comprising:

10   if the client computer does not have a pass to the website, randomly determining

if the client computer should be provided temporary access to the website instead of

setting the blocking layer over the website.

3.   The method of claim 1 further comprising:

      if the client computer has a pass to the website, allowing the end-user to interact

15   with the website instead of setting the blocking layer over the website.

4.   The method of claim 1 wherein at least a portion of the blocking layer is

transparent and allows viewing of portions of the website.

5.   The method of claim 1 wherein the blocking layer blocks a majority of the website

from view and prevents the end-user from interacting with any portion of the website.

20   6.   The method of claim 1 wherein the pass to the web site comprises a cookie.

7.   The method of claim 1 wherein searching the client computer for a pass to the website comprises looking for a cookie at the client computer and examining the cookie at the client computer.

8.   The method of claim 1 wherein the blocking layer allows the end-user to view a

5   portion of the website but does not allow the end-user to activate a link on that portion.

9.   The method of claim 1 further comprising:

if the client computer does not have a pass to the website, determining if the client computer is running a supported operating system; and

if the client computer is not running a supported operating system, providing the

10   client computer temporary access to the website instead of setting the blocking layer over the web site.

10.   The method of claim 1 further comprising:

if the client computer does not have a pass to the website, determining if the client computer is running a supported web browser; and

15   if the client computer is not running a supported web browser, providing the client computer temporary access to the website instead of setting the blocking layer over the web site.

11.   The method of claim 1 further comprising:

if the client computer does not have a pass to the website, displaying an offer to

20   gain access to the website; and

if the end-user does not accept the offer to gain access to the website, providing the client computer temporary access to the website.

12. The method of claim 1 further comprising:

if the client computer does not have a pass to the website, determining if cookies

5   are enabled in the client computer; and

if cookies are not enabled in the client computer, providing the client computer temporary access to the website instead of setting the blocking layer over the web site.

13. The method of claim 1 further comprising:

if the client computer does not have a pass to the web site, displaying an offer to

10   gain access to the website; and

if the end-user accepts the offer to gain access to the website, providing the client computer regular access to the web site.

14. A method of controlling access to a server computer, the method comprising:

receiving a request for a document from a client computer;

15   providing the document to the client computer;

determining if the client computer is authorized to access documents on the server computer; and

if the client computer is not authorized to access documents on the server computer, preventing an end-user on the client computer from interacting with the

20   document.

15. The method of claim 14 further comprising:

- 42 -

if the client computer is not authorized to access documents on the server computer, randomly determining if the client computer should be provided temporary access to documents on the server computer instead of preventing the end-user on the client computer from interacting with the document.

5   16.   The method of claim 14 wherein preventing the end-user from interacting with the document comprises displaying a blocking layer over the document.

17.   The method of claim 14 further comprising:

if the client computer is not authorized to access documents on the server computer, displaying a security prompt offering to gain access to documents on the

10   server computer; and

if the end-user does not accept the offer to gain access to documents on the server computer, providing the client computer temporary access to documents on the server computer.

18.   The method of claim 14 further comprising:

15   if the client computer is not authorized to access documents on the server computer, displaying a security prompt offering to gain access to documents on the server computer; and

if the end-user accepts the offer to gain access to documents on the server computer, providing the client computer regular access to documents on the server

20   computer.

19.   The method of claim 14 wherein the document comprises a web page and the server computer is hosting a website.

20.   A system for controlling access to a server computer, the system comprising:

a first server computer including a document downloadable over a computer network, the document including a reference to a filter code configured to determine if a client computer has a permission to access documents on a website;

5   a second server computer including a blocker code, the blocker code being configured to control access to documents on the website; and

a client computer configured to receive the document and the filter code, the filter code being configured to pull the blocker code from the second server computer to the client computer if the client computer does not have permission to access documents

10   on the website, the blocker code being configured to run in the client computer to block the computer from accessing documents on the website.

21.   The system of claim 20 wherein the blocker code is further configured to offer an end-user on the client computer regular access to documents on the website.

22.   The system of claim 20 wherein the filter code is further configured to randomly

15   determine whether to pull the blocker code instead of outright pulling the blocker code into the client computer.

23.   The system of claim 20 wherein the filter code is stored in the first server computer.

24.   The system of claim 20 wherein the documents comprise web pages and the

20   computer network comprises an Internet.